1. Účel směrnice

Tato směrnice (dále jen „Směrnice“) se vydává za účelem **technického a organizačního zajištění ochrany osobních, provozních a lokalizačních údajů** a **důvěrnosti komunikací** v souladu s požadavky § 88 zákona č. 127/2005 Sb., o elektronických komunikacích, (dále jen „Zákon“) a s ohledem na příslušná ustanovení zákona č. 110/2019 Sb., o zpracování osobních údajů a obecného nařízení o ochraně osobních údajů (GDPR).

2. Rozsah působnosti

1. Tato Směrnice se vztahuje na všechny zaměstnance, externí spolupracovníky a smluvní partnery společnosti [PLnet s.r.o.] (dále jen „společnost“), kteří se jakkoli podílejí na poskytování veřejně dostupné služby elektronických komunikací.

2. Směrnice je závazná pro všechny organizační složky společnosti, které zpracovávají, ukládají nebo jinak nakládají s osobními, provozními či lokalizačními údaji uživatelů.

3. Terminologie a definice

- **Osobní údaje**: ve smyslu GDPR, informace o identifikované nebo identifikovatelné fyzické osobě.
- **Provozní údaje**: údaje zpracovávané za účelem přenosu zpráv v síti elektronických komunikací.
- **Lokalizační údaje**: údaje zpracovávané v síti nebo službách elektronických komunikací, které udávají zeměpisnou polohu koncových zařízení uživatele.
- **Důvěrnost komunikací**: povinnost zajistit, aby obsah komunikací nebyl zpřístupněn neoprávněným osobám.

4. Organizační odpovědnosti

1. **Vedoucí představitel společnosti (Statutární orgán)**
   - Odpovídá za celkové nastavení bezpečnostní politiky a za zajištění zdrojů (personálních, finančních, technických) k její realizaci.
2. **Pověřenec pro ochranu osobních údajů (DPO), je-li jmenován**
   - Sleduje soulad s GDPR a dalšími předpisy upravujícími ochranu osobních údajů.
   - Radí společnosti ohledně posouzení dopadů na ochranu osobních údajů (DPIA), pokud je vyžadováno.
   - Projednává případné incidenty úniku osobních údajů a komunikuje s Úřadem pro ochranu osobních údajů (ÚOOÚ).
3. **IT manažer / Bezpečnostní manažer**
   - Odpovídá za implementaci a provoz technických opatření zabezpečujících data a komunikace (např. šifrování, přístupové kontroly atd.).
   - Provádí pravidelné testování bezpečnostních mechanismů a vyhodnocování rizik.
4. **Vedoucí jednotlivých oddělení**

- Zajišťují dodržování Směrnice v rámci svých týmů.
- V případě porušení Směrnice nebo bezpečnostního incidentu informují neprodleně IT manažera / Bezpečnostního manažera a DPO (pokud je jmenován).

5. Technická a organizační opatření (k § 88 odst. 1 písm. a))

1. **Řízení přístupů**
   - Zavádí se a pravidelně se reviduje systém oprávnění, aby k osobním, provozním a lokalizačním údajům měly přístup pouze osoby oprávněné a v nezbytném rozsahu.
2. **Šifrování**
   - Všechna citlivá data (např. databáze s osobními údaji, přenos dat mezi servery) musí být chráněna vhodnými kryptografickými metodami.
3. **Logování a monitorování**
   - Vedou se záznamy o přístupech k systémům obsahujícím osobní, provozní a lokalizační údaje.
   - Monitorují se podezřelé aktivity a včas se na ně reaguje.
4. **Zálohování a obnova**
   - Provádí se pravidelné zálohy klíčových systémů a databází.
   - Zajišťuje se bezpečné uložení záloh a ověřuje možnost obnovy dat (disaster recovery).
5. **Fyzická bezpečnost**
   - Zajišťuje se odpovídající ochranu serveroven, datových úložišť a dalších prostor, kde se vyskytují citlivá data (přístupové karty, kamerový systém, identifikace návštěv atd.).
6. **Kontrola dodavatelů**
   - Dodavatelské vztahy obsahují smluvní ujednání o ochraně a důvěrnosti údajů.
   - Pravidelně se vyhodnocuje, zda dodavatelé dodržují požadované standardy.

6. Interní procesy pro ochranu údajů (k § 88 odst. 1 písm. b))

1. **Vyhodnocení rizik**
   - Minimálně jednou ročně se provede analýzu rizik spojených se zpracováním osobních, provozních a lokalizačních údajů; následně se aktualizuje nebo doplní bezpečnostní opatření.
2. **Revize a aktualizace Směrnice**
   - Tato Směrnice podléhá pravidelné revizi (jednou ročně) a v případě právních nebo technologických změn je aktualizována.
3. **Školení zaměstnanců**
   - Zaměstnanci jsou školeni minimálně jednou ročně v oblasti bezpečnosti informací, ochrany osobních údajů a povinností vyplývajících ze Směrnice.
4. **Dokumentace a záznamy**

- Uchovává se veškerá relevantní dokumentace o ochranných opatřeních a rozhodnutích týkajících se zpracování údajů.

5. **Postup při změnách**

- Veškeré změny v informačních systémech a procesech týkající se zpracování osobních, provozních a lokalizačních údajů musí být dopředu vyhodnoceny z hlediska dopadu na bezpečnost a ochranu údajů.

7. Informování účastníků o rizicích (k § 88 odst. 1 písm. c))

1. Pokud je zjištěno **mimořádné bezpečnostní riziko** (např. nový typ útoku, technologická zranitelnost):

- Společnost je povinna na svých webových stránkách, případně prostřednictvím e-mailu či SMS, **informovat všechny dotčené uživatele**.

- V případě, že riziko přesahuje běžná opatření společnosti, informuje společnost uživatele o **možnostech, jak riziko minimalizovat**, a o případných nákladech, pokud je uživatel ponese sám.

2. V rámci ochrany dobrého jména a předejití dalším škodám je doporučeno srozumitelné a rychlé informování uživatelů všemi dostupnými kanály – toto podléhá vždy rozhodnutí statutárního orgánu.

8. Postupy pro vyřizování žádostí o přístup k osobním údajům (k § 88 odst. 1 písm. d))

1. **Příjem a evidence žádostí**

- Veškeré žádosti o přístup k osobním údajům (ať už od subjektů údajů, orgánů veřejné moci či dalších oprávněných osob) jsou evidovány.

2. **Ověření identity žadatele**

- Před poskytnutím osobních údajů se ověřuje identita žadatele a právní základ pro vyřízení žádosti (např. souhlas subjektu údajů, zákonná povinnost).

3. **Proces schválení**

- Je povinné posoudit každou žádost z hlediska zákonnosti (GDPR, Zákon, případně jiný právní předpis).

- Pokud je žádost v rozporu s právními předpisy, musí být zamítnuta a tato skutečnost řádně zdůvodněna.

4. **Lhůty pro vyřízení**

- Žádosti subjektů údajů musí být vyřízeny bez zbytečného odkladu, dle zákonných lhůt.

- Žádosti orgánů veřejné moci se řeší dle zákonných lhůt či dle urgentnosti spojené s povahou žádosti (např. trestní řízení).

5. **Reporting vůči ÚOOÚ**

- Na vyžádání poskytne společnost Úřadu pro ochranu osobních údajů informace o přijatých žádostech, jejich počtu, právním odůvodnění a způsobu vyřízení.

9. Kontrola, revize a sankce

1. **Interní audity**

   - Pravidelně (min. 1× ročně) se provádějí interní audity zaměřené na dodržování Směrnice a hodnotí se účinnost přijatých opatření.

2. **Externí kontroly a spolupráce s dozorovými orgány**

   - Společnost spolupracuje s Českým telekomunikačním úřadem (ČTÚ) a Úřadem pro ochranu osobních údajů (ÚOOÚ), kterým předkládá potřebné dokumenty a umožňuje provádění kontrol.

3. **Porušení povinností**

   - Každé porušení této Směrnice nebo relevantních právních předpisů může vést k pracovněprávním důsledkům a případně k sankcím dle vnitřních pravidel společnosti, zákoníku práce a dalších právních předpisů.

10. Závěrečná ustanovení

1. Tato Směrnice nabývá platnosti dnem [01.07.2025].

2. Veškeré doplňky nebo změny této Směrnice musejí být provedeny písemně a schváleny [jednatelem společnosti].

3. V případě rozporu mezi touto Směrnicí a platnými právními předpisy mají přednost právní předpisy.

Podpis odpovědné osoby:
[Radek Vychodil, jednatel společnosti PLnet s.r.o.]

Datum: …01.07.2025……